line 5, delete ",";

after line 15, as a separate line before line 16, insert the following heading:

--SUMMARY OF THE INVENTION--;

line 16, after "The" insert --present--; and replace "object of" with --need for--;

line 17, replace "using" with --with--;

delete lines 20-21 and insert the following:

--This need is met by an aspect of the present invention including a method for authenticating key devices using an asymmetric encryption method in which each key device is assigned a device-specific certificate. The method includes assigning each key device a group-specific signature key and also a group-specific signature of the device specific certificate. Furthermore, a group is comprised of a limited total number of key devices.

According to another aspect of the present invention, the group-specific signature key and the group-specific signature are allocated to each key device during a first initialization.

According to yet another aspect of the present invention, the steps of assigning the group-specific signature key and the group-specific signature of the device-specific certificate to an associated specific group is determined by comparing each key device with a stored list of approved key devices.

According to a further aspect of the present invention, a link is established between at least two key devices. A corresponding device-specific certificate and a corresponding device-specific signature key is transmitted from one of the key devices to another one of the key devices. Another one of the key devices then verifies authenticity of the corresponding device-specific certificate using the corresponding device-specific signature key according to the relationship:

D (S (Z (A)), pAD) = D (E (Z (A)), sAD), pAD) = Z (A)

where D represents a decryption function, S(Z(A)) represents signature of the corresponding device-specific certificate, E(Z(A)) represents an encryption function of the corresponding device-specific certificate, pAD represents a signature key of an administrator, sAD represents a secret key of the administrator and Z(A) represent the corresponding device-specific certificate.

Additional advantages and novel features of the present invention will be set forth, in part, in the description that follows and, in part, will become apparent to those skilled in the art upon examination of the following or may be learned by practice of the invention. The advantages of the invention may be realized and attained by means of the instrumentalities and combinations particularly pointed out in the appended claims.

A3

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS--;

~~lines~~ 23-24, replace "an exemplary embodiment" with --preferred embodiments--; and

~~line~~ 25, before ":" insert --that follows--.

On page 3:

~~line~~ 6, after "The" insert --present--;

replace line 11 with the following: --any other device and wherein the devices involved are--;

A4

~~line~~ 14, replace "per se, in practice" with --in the art--;

~~line~~ 15, replace "this" with --the corresponding--;

~~line~~ 18, after "the" insert --present--;

~~line~~ 22, delete ","; and after "be" (second occurrence) insert --stored--;

~~line~~ 23, replace ", for example" with --such as--;

~~line~~ 24, after "card" insert --, for example--; replace "Such a" with Each of the--; and replace "group" with --groups--;

~~line~~ 29, replace "per se" with --in the art--;

~~line~~ 31, replace ":" with --according to the relationship:--; and

after "sAD)" insert --.--.

On page 4:

~~line~~ 1, delete ",";

~~line~~ 2, replace ", in" with --within--;

replace line 3 with --The secret key (sAD, sX) and the public key--;

~~line~~ 4, replace "pAD, pX" with --(pAD, pX)--;

~~line~~ 5, replace "which" with --that--;

~~line~~ 10, replace "a refinement" with --an embodiment--;

~~line~~ 15, replace "him" with --the administrator--;

~~line~~ 18, replace ", that is to say" with --(i.e.,--;

line 19, after "devices" insert --)--;

line 20, delete ",";

line 22, replace ", that is to say" with --(i.e.,--;

line 23, replace "," with --)--;

line 24, replace ", that is to say" with --(i.e.,--;

line 25, replace ":" with --) according to the relationship:--;

line 26, replace "D (E (Z (A), sAD), pAD) = Z (A)" with --D (E (Z (A)), sAD), pAD) = Z (A).--;

line 29, replace "A" with --Hence,--; and

line 31, replace "can thus" with --, thus, can--.

On page 5:

line 2, delete ",";

line 7, delete ","; and

after line 8, insert the following paragraph:

While this invention has been described in connection with what are presently considered to be the most practical and preferred embodiments, it is to be understood that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

IN THE CLAIMS:

On page 6, replace "Patent Claims" with --What is claimed is:--.

Cancel claims 1-3 without prejudice or disclaimer.

Please add new claims 4-7 as follows.

4. A method for authenticating key devices using an asymmetric encryption method in which each key device is assigned a device-specific certificate, the method comprising the steps of:

assigning each key device a group-specific signature key; and

assigning each key device a group-specific signature of the device-specific certificate;

wherein a group is comprised of a limited total number of key devices.